UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/865,246	05/25/2001	Morton Gregory Swimmer	YOR920010310US1	3963

35526 7590 04/18/2006

DUKE. W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 04/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/865,246	SWIMMER ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *Appeal brief filed 01/30/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1-67 are pending.

Response to Applicant's Appeal Brief Arguments

4. Applicant's arguments with respect to the claims have been considered in an Appeal conference on 04/05/2006 but are moot in view of the new ground(s) of rejection. The finality of the rejection of the last Office action is withdrawn.

Claim Rejections - 35 USC § 102

5. **Claims 1-4, 6-7, 9-10, 13-20, 22-29, 31-32, 34-35, 38-45, 47-50, 52-53, 55-56** and **59-66** are rejected under 35 U.S.C. 102(b) as being anticipated by Dotan (5,822,517 A).

Applicant has described journaling on page 3 lines 8-9 of the specification in the "summary of the invention" as follows: "journaling involves storing a system state

before an action is executed so that the state can be restored upon demand". Applicant further described "the detection of the virus may be performed by using pattern matching on system audit trail in which system audit contain activities occurring within the data processing system" on the same page lines 9-11. Furthermore applicant described "journaled data" being used for the following reasons: "in response to an identification of the virus, the data is restored to its previous state using the journaled data" see page 3, lines 11-13. Therefore based on the above definition by applicant the following new ground of rejection has been rendered.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner

As per claims 1, 26 and 47 Dotan (5,822,517 A) teach a data processing system, a computer program product in a computer readable medium, a method in a data processing system for protecting data from damage **(see fig.3 & 4 and associated text where Dotan disclose method steps of 54 for protecting a program which corresponds to applicant's limitation "protecting data" by generating alarm in steps 64 of fig.3 & 4 and step 66 of fig.4 in order to protect the program from damage which corresponds to applicant's limitation "protecting data from damage" in relationship with data processing system of fig.1 and associated**

text which corresponds to applicant's limitation "data processing system") ,the system, means and method comprising:

Method steps and means and instructions Journaling the data to from journaled data **(see step 54 of fig.3 and 4 where the action of memorizing current program state as "initial program state" corresponds to Applicant's limitation "journaling data" that is storing the initial state of the data; see col.4, lines 27-35 where it disclose the act of storing the initial state of the program before execution which corresponds to applicant's "journaling data")**, wherein method steps and means and instructions journaling the data comprises maintaining a previous state of the data for subsequent, optional restore of the data to the previous state **(see abstract; fig.4, step 54 and associated text which corresponds to applicant's "maintaining a previous state" limitation since the initial state of the program is stored or memorized, and step 68 of fig.4 and associated text where the act of restore to initial state corresponds to applicant's limitation "optional restore of the data to the previous state")**; method steps and means and instructions for determining whether a virus is present in the data processing system after journaling of the data has began **(see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation "determining whether a virus present"; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps is a virus detection determination step),** method steps and means and instructions responsive to an

identification of the virus **(see step 64 of fig.4 and associated text where generating alarm corresponds to Applicant's "responsive to an identification of the virus"; col.7, lines 20-26)**, method steps and means and instructions restoring the data using the journaled data **(see step 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant "journaled data")**.

As per claims 13, 38 and 59 Dotan (5,822,517 A) teach a data processing system, a computer program product in a computer readable medium, a method in a data processing system for repairing damage to data **(see fig.3 & 4 and associated text where Dotan disclose method steps of 54 and 64-66 for protecting a program, restoring to initial state which corresponds to applicant's "repairing the damaged data in relationship with data processing system of fig.1 and associated text which corresponds to applicant's limitation "data processing system")**, the method, means and instructions comprising: saving a state of a data object in response to a request to access the data object by a process **(see step 54 of fig.3 and 4 where the action of memorizing current program state as "initial program state" corresponds to Applicant's limitation "saving a state of data object" that is storing the initial state of the data; see col.4, lines 27-35 where it disclose the act of storing the initial state; and step 52 of fig.4 and associated text corresponds to applicant's limitation "request to access"; also see col.4, lines 27-30),** method, means and instructions for performing pattern

matching of a set of actions taken within the data processing system **(see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation "performing pattern matching of set of actions"; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps)** and method, means and instructions for determining whether an unauthorized intrusion has occurred in response to performing pattern matching and if so **(see step 64 of fig.4 and associated text where generating alarm corresponds to Applicant's "responsive to an identification of the virus"; also see col.7, lines 20-26)** , method, means and instructions for initiation a rollback to return the data object back to its saved state **(see step 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant "rollback ...to its saved state")**.

As per claim 22 Dotan (5,822,517 A) teach an intrusion protection system for use in a data processing system **(see abstract; fig.1 and associated text; col.3, lines 44-67; col.4, lines 1-11 which disclose an intrusion detection system)** comprising: a sensor filter, wherein the sensor filter receives requests to access data within the data processing system from a process **(step 52 of fig.4 and associated text corresponds to applicant's above limitation; see col.6, lines 14-18; also see col.4, lines 27-30)**; a pattern matcher, wherein the pattern matcher receives actions initiated by the process, compares the actions to a pattern to form a comparison,

determines whether an unauthorized intrusion has occurred **(see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation determining whether an unauthorized intrusion present; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps is a virus detection determination step)**, generates a first indication in response to an identification of an absence of an unauthorized intrusion **(see step 62 of fig.4 and associated text where a matching disclose Applicant's above limitation; also see col.7, lines 20-26)**, and generates a second indication to restore the data to a prior state in response to an identification of the unauthorized intrusion **(see step 64 and 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant journaled data)**; and a journaler, wherein the journaler journals data in response to accessing of the data and restores the data to the prior state in response to the indication by the pattern matcher, wherein the data is journaled until the first indication is generated by the pattern matcher **(see step 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant journaled data)**.

As per claim 24 Dotan (5,822,517 A) teach a data processing system **(see fig.1 and associated text which corresponds to applicant's data processing system)** comprising: a bus system; a communications unit connected to the bus system; a

memory connected to the bus system **(see col.5, lines 57-67; col.6, lines 1-9 where it disclose the data processing system; communication unit, a bus system and connection between different devices through bus system is inherent features of a data processing system (please see any computer architecture books for meaning of the bus system and its relationship with other data system processing modules including the cpu). it is inherent where the cpu, memory I/O modules, controllers and other devices are communicate through bus system))**, wherein the memory includes as set of instructions **(see col.6, lines 1-12)**; and a processing unit connected to the bus system **(inherent part of data processing system)**, wherein the processing unit executes the set of instructions to journal the data to form journaled data **(see step 54 of fig.3 and 4 where the action of memorizing current program state as "initial program state" corresponds to Applicant's limitation "journaling data" that is storing the initial state of the data; see col.4, lines 27-35 where it disclose the act of storing the initial state of the program before execution which corresponds to applicant's "journaling data")**; determines whether a virus is present in the data processing system after journaling of data has begun **(see step 60 & 64 of fig.4 and associated text where generating alarm; col.7, lines 20-26 where it disclose detection of the virus)**; and restores the data using the journaled data in response to an identification of the virus **(see step 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant "journaled data")**.

As per claim 25 Dotan (5,822,517 A) teach a data processing system **(see fig.1 and associated text which corresponds to applicant's data processing system)** comprising: a bus system; a communications unit connected to the bus system; a memory connected to the bus system **(see col.5, lines 57-67; col.6, lines 1-9 where it disclose the data processing system; communication unit, a bus system and connection between different devices through bus system is inherent features of a data processing system (please see any computer architecture books for meaning of the bus system and its relationship with other data system processing modules including the cpu), it is inherent where the cpu, memory I/O modules, controllers and other devices are communicate through bus system)**, wherein the memory includes a set of instructions **(see col.6, lines 1-12)**; and a processing unit connected to the bus system **(inherent part of the data processing system)**, wherein the processing unit executes the set of instructions to save a state of a data object in response to a request to access the data object by a process **(see step 54 of fig.3 and 4 where the action of memorizing current program state as "initial program state" corresponds to Applicant's above limitation that is storing the initial state of the data; see col.4, lines 27-35 where it disclose the act of storing the initial state of the program)**; perform pattern matching of a set of actions taken within the data processing system **(see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation "performing pattern matching of set of**

actions"; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps); and determine whether an unauthorized intrusion has occurred in response to performing pattern matching **(see step 60, 64 associated text; col.7, lines 37-51 where it disclose determination, unauthorized intrusion has occurred which corresponds to applicant above limitation).**

As per claims 2, 27 and 48 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47 comprising: responsive to an absence of an identification of the virus, discarding the journaled data **(see step 60-62 where if no virus is found as the result of the matching, the program ends in fig.4 and associated text in relationship with col.6, lines 1-4 where the user input start the invocation of the program which corresponds to discarding the data if nothing found and save the final state as initial state for the next round of program invocation as disclosed in col.7).**

As per claims 3, 28 and 49 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the determining step comprises: performing pattern matching **(see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation "performing pattern matching of set of**

actions"; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps).

As per claims 4, 29 and 50 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 3, 28 and 49, wherein the performing step includes: comparing a set of actions occurring within the data processing system with a set of patterns **(see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation "performing pattern matching of set of actions"; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps)**.

As per claims 6, 31 and 52 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, further comprising: recording a sequence of actions occurring within the data processing system **(see step 54 of fig.4 and associated text where storing or memorizing the initial state corresponds to applicant's recording a sequence of actions limitation).**

As per claims 7, 32 and 53 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the data is data accessed by a process within the data

processing system **(see fig.2 in relationship with method steps of fig.3 or 4 and associated text where such access is being done within the computer of fig.2 which corresponds to applicant's above limitation).**

As per claims 9, 34 and 55 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47 further comprising: responsive to an identification of the virus, generating an indication halting a process accessing the data **(see fig.3 item 60 and 64 where by detecting the virus as applied to claim 1 above an alarm is being generated and the process is halted in step 62).**

As per claims 10, 35 and 56 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the data journaled is data accessed by a single process and maintained until a determination is made that the single process is eliminated as a virus candidate **(see as applied to claim 1 above, steps 60 and 62 of fig.4 and associated text where by matching the initial state and final state the process is end indicating elimination of a virus candidate or starting another process if such elimination is not done).**

As per claims 14, 39 and 60 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of

claims 13, 38 and 59, wherein the performing step comprises: comparing the set of actions to a pattern from a set of patterns to form a comparison; determining whether the comparison indicates that the unauthorized intrusion has occurred; and responsive to an absence of the unauthorized intrusion, repeating the comparing step using another pattern from the set of patterns **(see as applied to the independent claims above with respect to steps 52-66; col.6 which disclose this action is a continuation process for an invocation of access request)**.

As per claims 15, 40 and 61 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the performing step comprises: matching patterns with the set of actions; determining whether the unauthorized intrusion has occurred; if an intrusion is absent, determining whether a time threshold has been reached; and if an absence of a reaching of the time threshold is present, repeating the matching step using another set of actions **(see as applied to the independent claims above with respect to steps 52-66; col.6 which disclose this action is a continuation process for an invocation of access request; and the step 64 generating the alarm corresponds to applicant's threshold limitation)**.

As per claims 16, 41 and 62 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 14, 39 and 60, wherein match between the pattern and the set of actions

identifies an absence of the unauthorized intrusion **(see step 62 of fig.4 and associated text where a matching disclose Applicant's above limitation; also see col.7, lines 20-26)**.

As per claims 17, 42 and 63 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 14, 39 and 60, wherein match between the pattern and the set of actions identifies a presence of the unauthorized intrusion **(see step 60 and 64 of fig.4 and associated text; col.7).**

As per claims 18, 43 and 64 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the intrusion is caused by a virus **(see col.7, lines 52-66)**.

As per claims 19, 44 and 65 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the intrusion is caused by an authorized user input **(see col.6, lines 1-4)**.

As per claims 20, 45 and 66 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of

claims 13, 38 and 59 further comprising: saving a state of all data objects within the data processing system **(see step 54 of fig.4 and associated text; see col.6-7)**.

As per claim 23 Dotan (5,822,517 A) teach all limitation of the claims but do not disclose, wherein the intrusion protection system is located within an operating system **(see col.6, lines 8-13)**.

Claim Rejections - 35 USC § 103

6. **Claims 5, 8, 11, 12, 21,30, 33, 36, 37, 46, 51, 54, 57, 58 and 67** are rejected under 35 U.S.C. 103(a) as being unpatentable over Dotan (5,822,517 A) in view of Conklin et al (5,991,881 A).

As per claims 5, 21, 30, 46, 51 and 67 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26, 13, 38, 59 and 47 as applied to claim 1 above but do not explicitly disclose, wherein the data is located in a storage device external to the data processing system. However Conklin et al (5,991,881 A) disclose wherein the data is located in a storage device external to the data processing system **(see fig.3, 4 and associated text where the storage within the hosts are external to monitoring system)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Conklin's storage external device in Dotan's

software detection system in order to have no discemible address and can not be accessed by an intruder or hacker (see col.1, lines 66-67; col.2, lines 1-2).

As per claims 8, 33 and 54 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47 as applied above but do not explicitly disclose further comprising: responsive to an identification of the virus, blocking access to the data by a process accessing the data. However Conklin et al (5,991,881 A) disclose further comprising: responsive to an identification of the virus, blocking access to the data by a process accessing the data **(see col.5, lines 34-38)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Conklin's storage external device in Dotan's software detection system in order to have no discemible address and can not be accessed by an intruder or hacker (see col.1, lines 66-67; col.2, lines 1-2).

As per claims 11, 36 and 57 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47 as applied above but do not explicitly disclose, wherein the journaled data is stored in a protected memory accessible only by the method. However Conklin et al (5,991,881 A) disclose wherein the journaled data is stored in a protected memory accessible only by the method (see fig.9 and associated text). It would have been obvious to one of ordinary skilled in the art at the time the invention

was made to utilize Conklin's storage external device in Dotan's software detection system in order to have no discemible address and can not be accessed by an intruder or hacker (see col.1, lines 66-67; col.2, lines 1-2).

As per claims 12, 37 and 58 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 11, 37 and 57, but do not explicitly disclose wherein the journaled data is stored in a data structure located in a protected memory inaccessible by a process. However Conklin et al (5,991,881 A) disclose wherein the journaled data is stored in a data structure located in a protected memory inaccessible by a process (see fig.5 and associated text). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Conklin's storage external device in Dotan's software detection system in order to have no discemible address and can not be accessed by an intruder or hacker (see col.1, lines 66-67; col.2, lines 1-2).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Please see enclosed PTO-892.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 272-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

04/17/2006

AU 2132

Re-Open prosecution approved

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100